MAPPING SYSTEM AND CORRESPONDING METHOD TO REALIZE DIGITAL ASSETS ON THE MAPPING CHAIN BASED ON DISTRIBUTED TECHNOLOGY

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application claims priority of Chinese Invention Patent Application No. 201810339305.3 filed Apr. 16, 2018, which is incorporated herein by reference.

FIELD OF TECHNOLOGY

[0002] The present invention relates to the field of distributed technology, in particular to the field of blockchain technology, specifically, it refers to a mapping system and corresponding method to realize digital assets on the mapping chain based on distributed technology.

DESCRIPTION OF RELATED ARTS

[0003] Blockchain is essentially a decentralized database, it's like a shared ledger, records the transaction information of all encrypted digital assets, as the underlying technology of Bitcoin, blockchain has the characteristics of decentralization, openness, anonymity and non-tamperability.

[0004] The control right of encrypted digital assets is embodied in the control right of private key. Take Bitcoin as an example, the essence of private key is a random number, the private key algorithm of Bitcoin generates 256-bit random number by running SHA256 hash algorithm for random number. Add the version number in front, add compression mark and additional check code in the back (after two SHA-256 operations, take the first four bytes of the hash result twice), and then encode it with Base58, can get the private key in WIF (Wallet import Format) format. Public key is generates through secp256k1 elliptic curve algorithm, Bitcoin address is generates by the public key through hash function (RPIEMD+SHA).

[0005] At present, regardless of whether the encrypted digital assets in the hands of individuals or exchange, its private key are completely stored in a decentralized single point. This single point may be the user himself, or it may be a third party that provides a wallet or a decentralized exchange, etc. Therefore, various security issues such as the leakage, theft of private keys and malicious intrusion by third party frequently occur in the field of encrypted digital assets, particularly the encrypted digital asset exchanges have repeatedly occurred serious digital asset thefts event, causing huge losses in users' digital assets.

[0006] At the same time, mainstream blockchain networks such as Bitcoin and Ethereum are like islands and cannot communicate directly with each other, different blockchain encrypted digital assets held by users cannot be directly exchanged, that's greatly restricts the application of blockchain.

SUMMARY OF THE INVENTION

[0007] The object of the present invention is to overcome the drawbacks of the above prior arts, provides a mapping system and corresponding method to realize digital assets on mapping chain that can be mapped across chains based on distribute technology.

[0008] In order to achieve the above objects, the present invention of mapping system and corresponding method to realize digital assets on mapping chain based on distribute technology has the following composition:

[0009] The mapping system to realize digital assets on mapping chain bases on distribute technology, characterized in that, the said system comprises a mapping chain and at least two public chains, the mapping chain generates a private key sharing based on distribute technology and completes the decentralized custodial of each private key sharding, and by locking in and locking out the digital assets in at least the two public chains, to completes cross-chain communication between at least the two public chains.

[0010] The method to realize locking in and controlling of digital assets based on the above system, characterized in that, the said method comprises:

[0011] (A1) sending a request for locking in the digital asset in a public chain, and triggering a smart contract on the mapping chain for locking in the digital assets;

[0012] (A2) the mapping chain generates a private key sharding based on distributed technology, and completes the decentralized custodial of each private key sharding;

[0013] (A3) the public chain transfers control right of the digital assets to the mapping chain, in order to realize the distributed management of the digital asset;

[0014] (A4) confirming the successfully transferring of control right of the digital assets, and then the smart contract updates the account status of the mapping chain, in order to complete locking in and mapping of the digital assets.

[0015] In step (A2) of the method to realize locking in and controlling of digital assets, the mapping chain generates the private key sharding based on the distributed key generation protocol DKG, and to decentralized custodial of each private key sharding.

[0016] The method to realize locking in and controlling of digital assets, the decentralized custodial of each private key sharding is specifically:

[0017] saving each private key sharding in each node of the mapping chain.

[0018] In step (A3) of the method to realize locking in and controlling of digital assets comprises:

[0019] (A31) the mapping chain generates a locked address of the public chain based on each private key sharding;

[0020] (A32) transferring the digital assets to the locked address, and initiate a transaction broadcast to the mapping chain of transferring the digital assets;

[0021] (A33) through the query interface, each node of the mapping chain confirms that the transaction of the digital assets is confirmed on the public chain, and then transfers the control right of the digital assets for which transaction has been completed.

[0022] The method to realize locking out and controlling of digital assets based on the above system, characterized in that, the said method comprises:

[0023] (B1) initiating a request for locking out in the digital assets in a public chain, in order to trigger a smart contract on the mapping chain for locking out the digital assets;

[0024] (B2) each node in the mapping chain respectively receives transaction broadcast information generated based on the triggered smart contract, and completes the transaction of the digital assets when the transaction signature of each the said node reaches threshold value of transaction signature;